




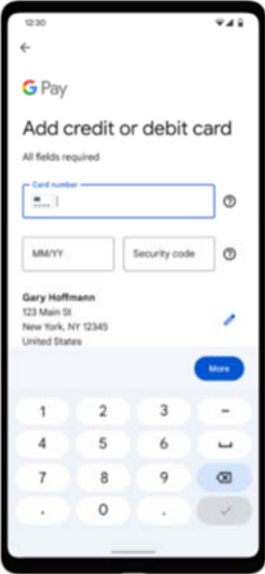
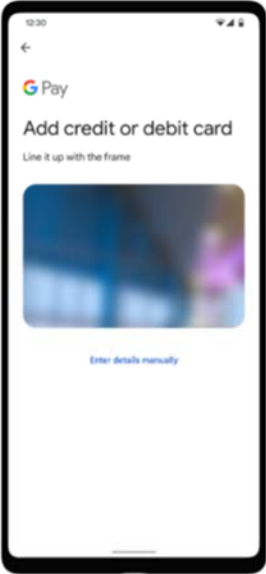
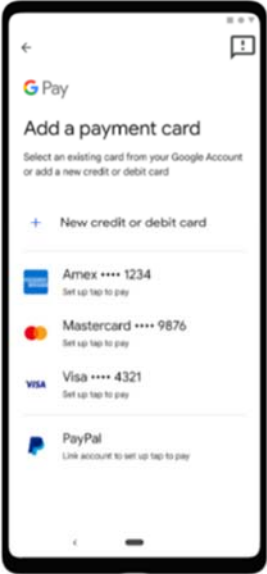



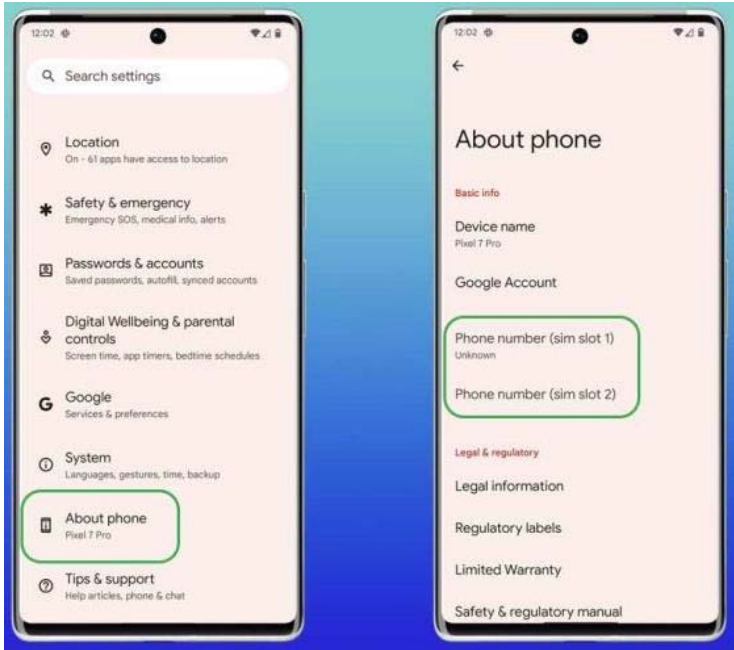
Exhibit E

Exhibit E - U.S. Patent No. 10,339,520

Claim No.	Google Pay- and/or Google Wallet-Enabled Computing Device
<p>10 [Pre]: A method of storing and generating payment information in an electronic device, the method comprising:</p>	<p>A Google Pay and/or Google Wallet-enabled computing device is an electronic device that practices a method of storing and generating payment information.</p> <div data-bbox="489 362 884 745">  </div> <div data-bbox="888 362 1346 745"> <h3>Takeaways</h3> <ul style="list-style-type: none"> Pixel is powered by all the smarts of Google, including the Tensor chip Ask Google Assistant to make a call from your Pixel Buds, so you can keep your hands free¹ Google apps come loaded on every Pixel, including Google Maps to help you get to your destination,² and Google Wallet to give you an easy way to pay when you arrive³ </div> <h2>Get help paying the tab</h2> <p>[. . .]</p> <p>Knox picked up the bill and paid with Google Wallet, which lets you store your credit and debit cards and pay quickly from your Pixel phone or Pixel Watch.³</p> <p>See, e.g., <i>An even better way to use your favorite Google apps.</i>, Google, https://store.google.com/intl/en/ideas/articles/google-software-features/; <i>Install and update apps on Google Pixel Watch</i>, Google, https://support.google.com/googlepixelwatch/answer/13044412 (“Google Pixel Watch 2 is preloaded with more apps like Calendar, Fitbit, Google Wallet, Google Maps, YouTube Music and more.”); <i>Google Wallet</i>, Google, https://wallet.google/.</p> <div data-bbox="489 1101 1738 1390"> <div>  <h2>Tap to pay for everyday essentials</h2> <p>Your phone is now your wallet—just unlock, tap, and look for the check mark.</p> </div> <div>  <h2>Seamless online checkout</h2> <p>Google Pay is your online checkout companion. Pay safely in fewer steps.</p> </div> </div> <p>See, e.g., <i>Google Pay – Pay In Store</i>, Google, https://pay.google.com/about/pay-in-store/; <i>Google Pay – Pay Online</i>, Google, https://pay.google.com/about/pay-online/.</p>

Claim No.	Google Pay- and/or Google Wallet-Enabled Computing Device
	<p>Device tokenization</p> <p>When a user successfully adds their card to Google Pay, Google Pay stores a uniquely generated token on the device that has its own value. This new number, called a dynamic primary account number (DPAN) or device token, is similar to a credit card number.</p> <p>A DPAN improves account security because Google Pay passes it to a terminal during payment instead of the actual card number. In Google Pay, DPAN is referred as a 'virtual account number'. Users can only see the last four digits of this number, which are visible on the card details view in the Google Wallet app.</p> <p><i>See, e.g., Google Pay – Device Tokenization – TSP Integration</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview; <i>Google Pay – Device Tokenization – Overview</i>, Google (Oct. 16, 2024), https://developers.google.com/pay/issuers.</p> <p>Highlights of Google Pay's security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token's DPAN rather than the FPAN of the card. This "tokenization" provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder's mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p><i>See, e.g., Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Payment data cryptography for merchants</i>, Google Pay for Payments – Android (Oct. 24, 2024), https://developers.google.com/pay/api/android/guides/resources/payment-data-cryptography.</p>
10[a]: accepting a user input of issued payment information input at a touch screen display of the electronic device, wherein the information comprises an issuer provided payment information;	<p>A Google Pay- and/or Google Wallet-enabled computing device accepts a user input of issued payment information input at a touch screen display of the electronic device, wherein the information comprises an issuer provided payment information.</p> <p>Add new card</p> <p>With the Google Wallet app </p> <ol style="list-style-type: none"> 1. Open the Google Wallet app . 2. At the bottom, tap Add to Wallet +. 3. Tap Payment card. <ul style="list-style-type: none"> • Any cards you saved to your Google Account are shown. 4. Tap New credit or debit card. <ul style="list-style-type: none"> • To add a card, use your camera or tap Enter details manually. 5. At the bottom, tap Save and continue. <p><i>See, e.g., Add a new debit or credit card</i>, Google Wallet Help, https://support.google.com/wallet/answer/12058983; <i>Make contactless payments with Google Pixel Watch</i>, Google Pixel Watch Help, https://support.google.com/googlepixelwatch/answer/12661007.</p>


Claim No.	Google Pay- and/or Google Wallet-Enabled Computing Device
	<div><div>Key Google Pay UX flows</div><div><p>Cards can be added to Google Pay either through Google Wallet surfaces or an issuer's mobile banking app using the Push Provisioning API. Google Wallet app surfaces let users to enter their card details in multiple ways, including autofilling the details using a card already stored on file, OCR scanning, and manual entry.</p></div><div><div></div><div><div>Card on File</div><div>OCR Scanning</div><div>Manual entry</div></div><div><p>See, e.g., <i>Google Pay – Device Tokenization – TSP Integration – Google Pay Flows</i>, Google (May 2, 2024), https://developers.google.com/pay/issuers/tsp-integration/gpay-flows.</p></div><div><div>Add a card to your Google Wallet</div><div></div><div><div>Add a credit or debit card</div><div><p>If you add a card to your watch, you don't need your phone to pay.</p><ol style="list-style-type: none">1. On your smartwatch, open the Google Wallet app 🇵🇸.2. Tap Get started.3. Set up screen lock if you haven't already.4. On your phone, follow the instructions to add a Suica, credit, or debit card.<div>Tip:</div><ul style="list-style-type: none">• This only adds a card to the Google Wallet app on your watch, not your phone.</div><div><p>See, e.g., <i>Make contactless payments with Google Pixel Watch</i>, Google, https://support.google.com/googlepixelwatch/answer/12661007?hl=en.</p></div></div></div></div></div>

Claim No.	Google Pay- and/or Google Wallet-Enabled Computing Device
<p>10[b]: wherein the electronic device comprises device-specific and user-specific information; and</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device comprises device-specific and user-specific information.</p> <p>Add a Google or other account to your phone</p> <ol style="list-style-type: none"> 1. Open your device's Settings app. 2. Tap Passwords & accounts. 3. Under "Accounts," tap Add account. 4. Tap the type of account you want to add. <ul style="list-style-type: none"> • To add your Google Account, tap Google. When you sign in with a Google Account, the email, contacts, calendar events, and other data associated with that account automatically sync with your device. • To add your Google Meet account, tap Meet. When you sign in with your Meet account, you can make and receive video calls, create meetings, and call devices linked to your Home. <p><i>See, e.g., Add or remove Google & other accounts on your Pixel phone, Pixel Phone Help, https://support.google.com/pixelphone/answer/2840815; Fix account and password issues for Pixel Watch, Google Pixel Watch Help, https://support.google.com/googlepixelwatch/answer/13579196.</i></p>  <p><i>See, e.g., Andrew Romero, How to find you phone number on Android devices, 9 To 5 Google (May 9, 2023 9:14 am PT), https://9to5google.com/2023/05/09/find-phone-number/; Find your device serial number, Google Store Help, https://support.google.com/store/answer/3333000.</i></p>

Claim No.	Google Pay- and/or Google Wallet-Enabled Computing Device
10[c]: wherein the issuer provided payment information is communicated wirelessly; and	<p>A Google Pay- and/or Google Wallet-enabled computing device wirelessly communicates issuer-provided payment information.</p> <p>The following flow diagrams show how the cardholder's device, Google's servers, the TSP, and the card issuing bank's systems interact to provision a token.</p> <pre>sequenceDiagram participant User participant Google participant TSP participant Issuer User->>Google: User enters card details User->>Google: User accepts Google Pay ToS Google->>TSP: checkEligibility() TSP->>Issuer: checkEligibility() Issuer-->>TSP: Success TSP-->>Google: Success (card metadata, Issuer ToS, card art) Google->>User: Present issuer ToS User->>Google: ToS accpeted Google->>TSP: tokenize(risk signals, provisioning data) TSP->>Issuer: tokenize(risk signals, provisioning data) Issuer-->>TSP: idvOutcome(approved, declined,challenge) TSP-->>Google: idvOutcome(approved, declined,challenge) Google->>User: idvOutcome(approved, declined,challenge) Note over User,Google,TSP,Issuer: If ID&V outcome="green", flow complete, active token. Note over User,Google,TSP,Issuer: If ID&V outcome="red", flow complete, no token. Note over User,Google,TSP,Issuer: If ID&V outcome="yellow", proceed to ID&V. SMS example below.</pre> <p>See, e.g., <i>Google Pay – Device Tokenization – TSP Integration – Overview</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview; <i>Google Pay FAQ</i>, Aerospace Federal Credit Union, https://www.aerofcu.org/Services/Digital-Wallet/Google-Pay-FAQ (“[Google Pay] requires an active Internet connection when adding or removing a payment card or to download transaction history. You can connect via a Wi-Fi network or using your mobile data connection.”).</p>

Claim No.	Google Pay- and/or Google Wallet-Enabled Computing Device
<p>10[d]: receiving wirelessly a static device account number payment information for storage on the electronic device; and</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device wirelessly receives a static device account number payment information for storage on the electronic device.</p> <p>12) Will the DPAN be stored encrypted along with the LUK in the service layer's sqlite database?</p> <p>Yes. Each TSP provides a payment bundle which includes static data like the token and dynamic data like the keys. The bundle data is stored encrypted on the device.</p> <p><i>See, e.g., Google, Google Pay Security Paper (Ver. 2.4, Jan. 2022) available at https://developers.google.com/wallet/access/campus-id/resources/Google_Pay_Security_Paper_2.4.pdf.</i></p> <p>Device tokenization</p> <p>When a user successfully adds their card to Google Pay, Google Pay stores a uniquely generated token on the device that has its own value. This new number, called a dynamic primary account number (DPAN) or device token, is similar to a credit card number.</p> <p>A DPAN improves account security because Google Pay passes it to a terminal during payment instead of the actual card number. In Google Pay, DPAN is referred as a 'virtual account number'. Users can only see the last four digits of this number, which are visible on the card details view in the Google Wallet app.</p>

Claim No.	Google Pay- and/or Google Wallet-Enabled Computing Device
	<p>The following flow diagrams show how the cardholder's device, Google's servers, the TSP, and the card issuing bank's systems interact to provision a token.</p> <pre>sequenceDiagram participant User participant Google participant TSP participant Issuer User->>User: User enters card details User->>Google: User accepts Google Pay ToS Google->>TSP: checkEligibility() TSP->>Issuer: checkEligibility() Issuer-->>TSP: Success TSP->>Google: Success (card metadata, Issuer ToS, card art) Google->>User: Present issuer ToS User->>Google: ToS accpeted Google->>TSP: tokenize(risk signals, provisioning data) TSP->>Issuer: tokenize(risk signals, provisioning data) Issuer-->>TSP: idvOutcome(approved, declined, challenge) TSP->>Google: idvOutcome(approved, declined, challenge) Google->>User: idvOutcome(approved, declined, challenge) Note over User, Google, TSP, Issuer: If ID&V outcome="green", flow complete, active token. Note over User, Google, TSP, Issuer: If ID&V outcome="red", flow complete, no token. Note over User, Google, TSP, Issuer: If ID&V outcome="yellow", proceed to ID&V. SMS example below.</pre> <p>See, e.g., <i>Google Pay – Device Tokenization – TSP Integration – Overview</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview; <i>Google Pay FAQ</i>, Aerospace Federal Credit Union, https://www.aerofcu.org/Services/Digital-Wallet/Google-Pay-FAQ (“[Google Pay] requires an active Internet connection when adding or removing a payment card or to download transaction history. You can connect via a Wi-Fi network or using your mobile data connection.”).</p>

Claim No.	Google Pay- and/or Google Wallet-Enabled Computing Device
<p>10[e]: wherein at least a portion of the payment information is a limited use number for limited use by the device, in place of a issuer provided payment information; and,</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device generates payment information, at least a portion of which is a limited use number for limited use by the device, in place of a issuer provided payment information.</p> <p>Tokens and cards-on-file</p> <p>When a user adds their card to Google Pay, they get one or more of the following:</p> <ul style="list-style-type: none"> • Device token (DPANs) • Card-on-file (PAN/FPAN, expiry, and cardholder name) • Cloud token (tokenized version of a card-on-file) <p>Device tokens, cards on file, and cloud tokens are used in different scenarios. Device tokens are device bound and can be used for in-store NFC transactions and online transactions. Cards on file and cloud tokens are stored at the account level, rather than on the device, and can be used for peer-to-peer and online transactions. When tokenizing a card, the user's card information may be stored as a card on file and can potentially incur a small, temporary charge. This charge is refunded once the account has been verified. More information can be found on the Google charge support page </p> <p><i>See, e.g., Google Pay – Device Tokenization – Overview</i>, Google (Oct. 16, 2024), https://developers.google.com/pay/issuers; <i>Google Pay – Device Tokenization – TSP Integration</i>, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview; <i>Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security.</p> <p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant's acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay's security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token's DPAN rather than the FPAN of the card. This "tokenization" provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder's mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p><i>See, e.g., Google Pay – Device Tokenization – Security</i>, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; <i>Payment data cryptography for merchants</i>, Google Pay for Payments – Android (Oct. 28, 2024), https://developers.google.com/pay/api/android/guides/resources/payment-data-cryptography.</p>

Claim No.	Google Pay- and/or Google Wallet-Enabled Computing Device
<p>10[f]: dynamically generating a one-time limited-use number based on at least one of a set of information including: user-identifying information; user secrets; device information; device secrets; time; merchant; facility location; sequence count; payment information; account information; amount; and transaction information; and</p>	<p>A Google Pay- and/or Google Wallet-enabled computing device dynamically generates a one-time limited-use number based on at least one of a set of information including: user-identifying information; user secrets; device information; device secrets; time; merchant; facility location; sequence count; payment information; account information; amount; and transaction information.</p> <p>5.0 Secure Limited-Use Key Storage</p> <p>5.1 Context</p> <p>Conventional provisioning of credit card information to a device (whether tokenized or not) involves storing a Master Key on a trusted piece of hardware like a Secure Element. For the purpose of this document, it will be called Card Master Key (CMK). CMK is synonymous with Master Derivation Key (MDK).</p> <p>The CMK serves as a long-term secret used to compute cryptographic dynamic verification codes (CVC3) are generated for MSD transactions and ARQC (Online Authorization Request) cryptograms are generated for EMV transactions. These are verified by the issuer during issuer authorization.</p> <p><i>See, e.g., Google, Google Pay Security Paper (Ver. 2.4, Jan. 2022) available at https://developers.google.com/wallet/access/campus-id/resources/Google_Pay_Security_Paper_2.4.pdf; Google Pay – Device Tokenization – Security, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; Payment data cryptography for merchants, Google Pay for Payments (Oct. 28, 2024), https://developers.google.com/pay/api/android/guides/resources/payment-data-cryptography.</i></p> <p>8 Application Cryptogram and Issuer Authentication</p> <p>The aim of this section is to provide methods for the generation of the Application Cryptograms (TC, ARQC, or AAC) generated by the ICC and the Authorisation Response Cryptogram (ARPC) generated by the issuer and verified by the ICC. For more details on the role of these cryptograms in a transaction, see section 10.8 of Book 3.</p> <p>[. . .]</p>

Claim No.	Google Pay- and/or Google Wallet-Enabled Computing Device																						
	<p>8.1 Application Cryptogram Generation</p> <p>8.1.1 Data Selection [. . .]</p> <p>The recommended minimum set of data elements to be included in Application Cryptogram generation is specified in Table 26.</p> <table border="1"> <thead> <tr> <th>Value</th><th>Source</th></tr> </thead> <tbody> <tr> <td>Amount, Authorised (Numeric)</td><td>Terminal</td></tr> <tr> <td>Amount, Other (Numeric)</td><td>Terminal</td></tr> <tr> <td>Terminal Country Code</td><td>Terminal</td></tr> <tr> <td>Terminal Verification Results</td><td>Terminal</td></tr> <tr> <td>Transaction Currency Code</td><td>Terminal</td></tr> <tr> <td>Transaction Date</td><td>Terminal</td></tr> <tr> <td>Transaction Type</td><td>Terminal</td></tr> <tr> <td>Unpredictable Number</td><td>Terminal</td></tr> <tr> <td>Application Interchange Profile</td><td>ICC</td></tr> <tr> <td>Application Transaction Counter</td><td>ICC</td></tr> </tbody> </table> <p>Table 26: Recommended Minimum Set of Data Elements for Application Cryptogram Generation</p> <p><i>See, e.g., EMVCo, EMV Integrated Circuit Card Specifications for Payment Systems, Book 2 – Security and Key Management v4.3 at 11, 21, 87–88 (Nov. 2011), available at https://www.emvco.com/emv-technologies/payment-tokenisation/.</i></p>	Value	Source	Amount, Authorised (Numeric)	Terminal	Amount, Other (Numeric)	Terminal	Terminal Country Code	Terminal	Terminal Verification Results	Terminal	Transaction Currency Code	Terminal	Transaction Date	Terminal	Transaction Type	Terminal	Unpredictable Number	Terminal	Application Interchange Profile	ICC	Application Transaction Counter	ICC
Value	Source																						
Amount, Authorised (Numeric)	Terminal																						
Amount, Other (Numeric)	Terminal																						
Terminal Country Code	Terminal																						
Terminal Verification Results	Terminal																						
Transaction Currency Code	Terminal																						
Transaction Date	Terminal																						
Transaction Type	Terminal																						
Unpredictable Number	Terminal																						
Application Interchange Profile	ICC																						
Application Transaction Counter	ICC																						
10[g]: using said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction.	<p>The Google Pay and/or Google Wallet-enabled computing device uses said static device account number and said dynamically generated one-time limited-use number together in the place of issuer provided payment information for making a payment transaction.</p> <p>Google Pay was designed to provide the flexibility required for an open platform and protection for all users: the cardholder, merchant, network, the merchant's acquiring bank, and the card issuing bank.</p> <p>Highlights of Google Pay's security features include:</p> <ul style="list-style-type: none"> • Network tokenization standards: When a cardholder makes a purchase using a device token, Google Pay sends the token's DPAN rather than the FPAN of the card. This "tokenization" provides your cardholders with an extra layer of security. • Secure in-memory storage of limited-use keys (LUKs): Your cardholder's mobile device stores the primary key that generates transaction cryptograms for contactless transactions. No other primary key data is stored on the device. <p><i>See, e.g., Google Pay – Device Tokenization – Security, Google (Sept. 12, 2024), https://developers.google.com/pay/issuers/overview/security; Google Pay – Device Tokenization – TSP Integration, Google (Feb. 1, 2024), https://developers.google.com/pay/issuers/tsp-integration/overview.</i></p>																						

Claim No.	Google Pay- and/or Google Wallet-Enabled Computing Device
	<p data-bbox="489 204 1501 240">At a high level, the Google Pay security approach: [. . .]</p> <ul data-bbox="527 245 1381 358" style="list-style-type: none"><li data-bbox="527 245 1381 302">• Adheres to standards for payment network tokenization, the creation and use of a cryptogram to represent payment credentials.<li data-bbox="527 306 1381 358">• Unlocks these cryptograms with limited-use keys (LUKs) or single use keys (SUKs), which are stored in-memory on the device. <p data-bbox="489 370 1703 427"><i>See, e.g., Google, Google Pay Security Paper (Ver. 2.4, Jan. 2022) available at https://developers.google.com/wallet/access/campus-id/resources/Google_Pay_Security_Paper_2.4.pdf.</i></p>